Security In A Connected World

David B. Nelson, Ph.D., CISSP

Director

National Coordination Office for

Information Technology Research and Development

SURA/CIPP Cybersecurity Symposium

George Mason Law School

March 8, 2004

Federal Networking and Information Technology Research and Development Program (NITRD)

- Coordinates and focuses interagency IT R&D:
  - Identify common research needs
  - Plan inter-agency research programs
  - Coordinate research announcements and funding
  - Review research results and adjust accordingly
- Evolved from the Federal High Performance Computing and Communications Initiative (HPCC), Computing Information and Communications Program (CIC), and Next Generation Internet Program (NGI)
- Includes 14 federal agencies, about $2B budget
- Cybersecurity will be cross-cutting special topic this year
- www.nitrd.gov

Participating Agencies and Departments

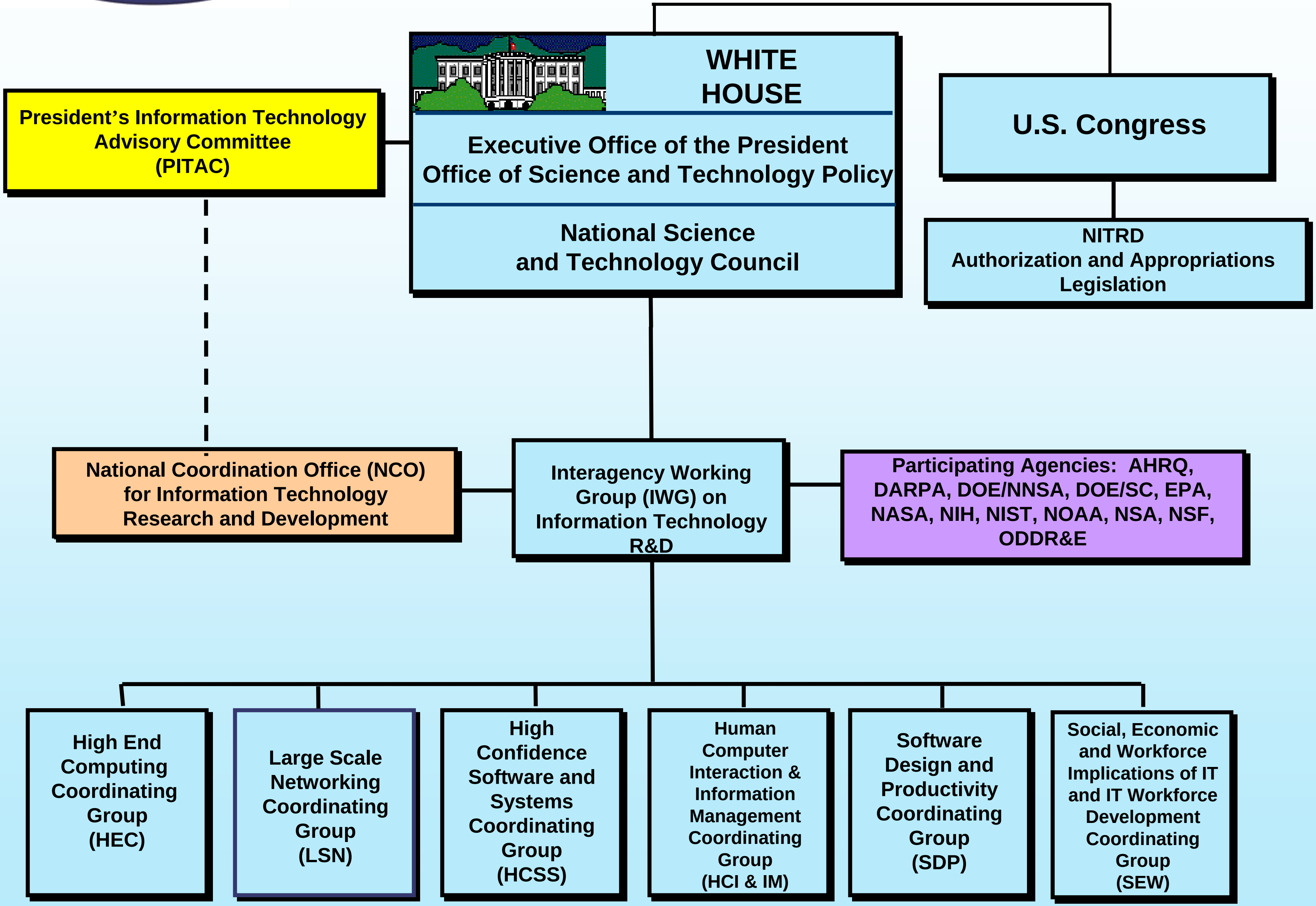
- Department of Defense
  - Defense Advanced Research Projects Agency (DARPA)
  - Defense Information Systems Agency (DISA)
  - National Security Agency (NSA)
  - Office of the Director of Defense Research and Engineering (ODDR&E)
- Department of Energy
  - Office of Science (DOE/SC)
  - National Nuclear Security Administration (DOE/NNSA)
- Department of Health and Human Services
  - National Institutes of Health (NIH)
  - Agency for Health Research and Quality (AHRQ)
- Department of Commerce
  - National Institute of Standards and Technology (NIST)
  - National Oceanic and Atmospheric Administration (NOAA)
- National Science Foundation (NSF)
- National Aeronautics and Space Administration (NASA)
- Environmental Protection Agency (EPA)
- Observer: Federal Aviation Administration (FAA)

National Coordination Office (NCO) for Information Technology Research and Development

Mission: *To formulate and promote Federal information technology research and development to meet national goals.*

- Part of National Science and Technology Council in White House
- Coordinates NITRD program planning, budget, and assessment
- Supports Interagency Working Group and six technical Coordinating Groups
- Supports the President's Information Technology Advisory Committee (PITAC)
  - Cybersecurity review
- Director of NCO reports to Director, Office of Science and Technology Policy and co-chairs Interagency Working Group

NITRD Program Coordination



WHITE HOUSE

Executive Office of the President
Office of Science and Technology Policy

National Science and Technology Council

President's Information Technology Advisory Committee (PITAC)

U.S. Congress

NITRD Authorization and Appropriations Legislation

National Coordination Office (NCO) for Information Technology Research and Development

Interagency Working Group (IWG) on Information Technology R&D

Participating Agencies: AHRQ, DARPA, DOE/NNSA, DOE/SC, EPA, NASA, NIH, NIST, NOAA, NSA, NSF, ODDR&E

High End Computing Coordinating Group (HEC)

Large Scale Networking Coordinating Group (LSN)

High Confidence Software and Systems Coordinating Group (HCSS)

Human Computer Interaction & Information Management Coordinating Group (HCI & IM)

Software Design and Productivity Coordinating Group (SDP)

Social, Economic and Workforce Implications of IT and IT Workforce Development Coordinating Group (SEW)

Other Government Organizations Relevant to Cyber-Security Research

- **Infosec Research Council**
  - Mostly Defense Community
  - Infosec Hard Problems List
- **Critical Information Infrastructure Protection Interagency Working Group**
  - Beginning work on research priorities
- **President's Information Technology Advisory Committee**
  - Addressed later in this talk
- **Federal research-funding agencies**
  - NSF solicitation (see Carl Landwehr's talk)

Likely Characteristics of Future Computing Environment

- **Critical to the Enterprise**
  - Agent for most business processes
  - More robust and self-regulating
  - Essential for *functions* as well as data
    - Process control, embedded computing, Supervisory Control and Data Acquisition (SCADA)
- **Connected: extends beyond organizational boundaries**
  - Virtual organizations
  - Membership and trust issues: people and systems
- **Widely Distributed**
  - "The network is the computer" - Scott McNealy
  - Modularized through middleware: Grid services, Web services, collaboration tools
  - Computing on demand using remote resources
  - Remote monitoring, control and coordination of processes

Likely Characteristics of Future Computing Environment

- **Ubiquitous and Dynamic**
  - Always available by wireless and wired connections
  - Portable identity and workspace
  - Human-centric with improved collaboration, communication, and resource discovery tools
  - Management and configuration issues
- **Heterogeneous**
  - Many different kinds of devices with different function, power and characteristics
  - Alternative technologies for organization/presentation of data
- **Challenging to maintain security**
  - Hard to determine what is inside vs. outside
  - Hard to determine appropriate usage/users for identity, authentication, authorization
  - Web Services will mean port 80 is used for “everything”
  - Increasing demands for privacy and anonymity
  - Need for role-based security

Security Concerns Are Also Evolving

- **Classic security concerns dealt more with data**
  - Confidentiality (Data only available to those authorized)
  - Availability (Data is available when you want it)
  - Integrity (Data hasn’t been changed)
- **Newer concerns deal more with people, transactions and functions**
  - Trust (Who you are and what you are authorized to do; either as person or system)
  - Non-repudiation (You can’t deny doing something you did)
  - Auditability (I can check what you did)
  - Reliability and predictability (The system does what what it should do)
  - Privacy (Within certain limits no one should know who I am or what I do)
- **Some solutions in stand-alone mainframe environment are less effective in networked environment**

Security Challenges of Future Computing Environment

- How to accommodate vision of distributed large-scale collaborations, access to resources, eCommerce, without compromising security?
- How to accommodate dynamic computing environment within current framework of security risk management?
- How to evolve security practices and technologies to keep up with future computing environment?
- How to build security into architecture of future environment, including ability to withstand, identify, and respond to attacks?
- How to say “yes” rather than “no” to users and developers without compromising security?

Computer Research Association Workshop Vision of Alternate Futures*

- Overwhelming unsolicited junk
- Rampant ID theft
- Frequent network outages
- Frequent manual intervention
- Largely unchecked abuses of laws and rights

- No spam or viruses
- User-controlled privacy
- Uninterrupted communications
- “Hassle-free” computing
- Balanced regulation and law-enforcement

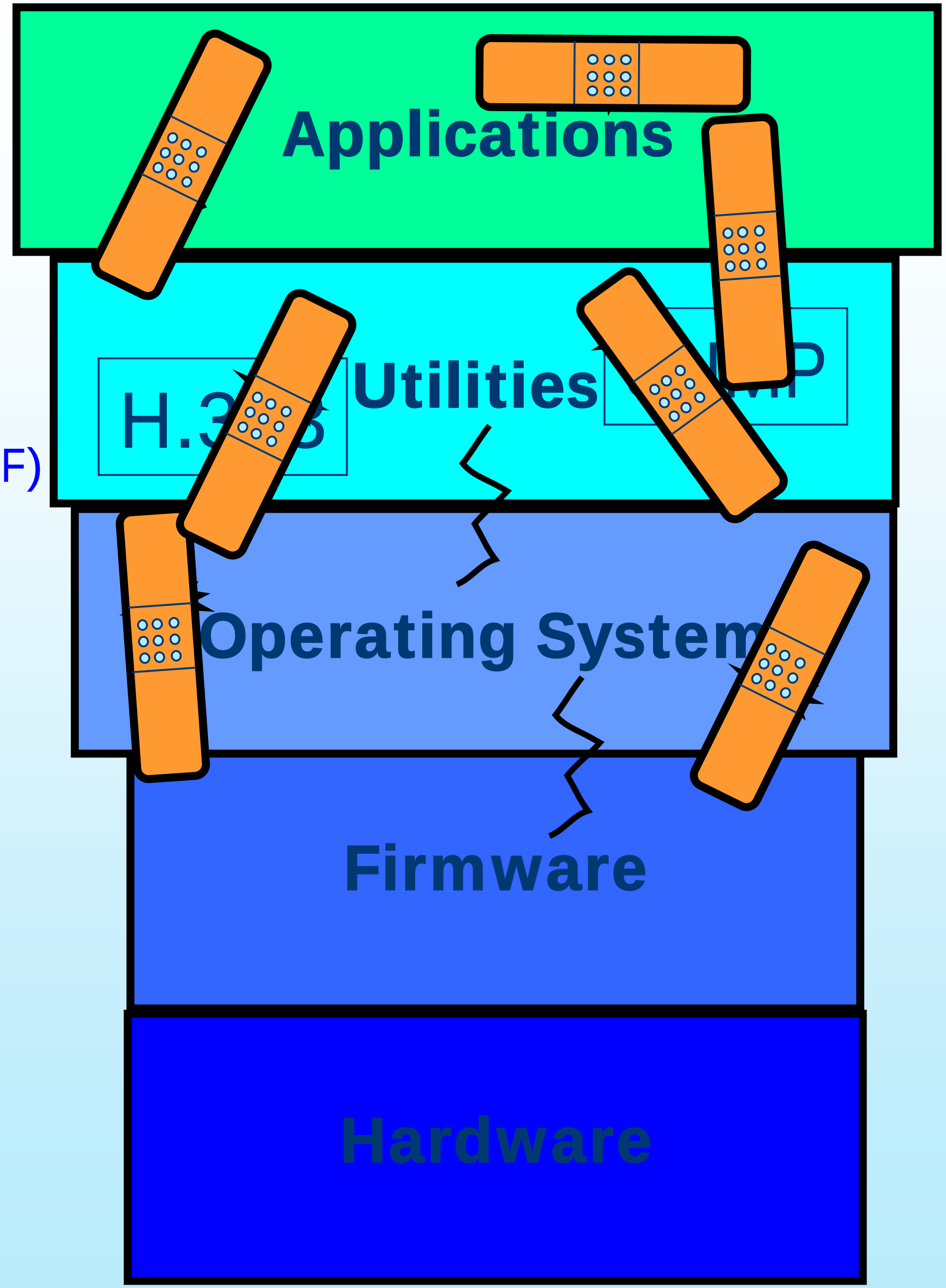
*http://www.cra.org/Activities/grand.challenges/security/slides.pdf

What’s the Problem?

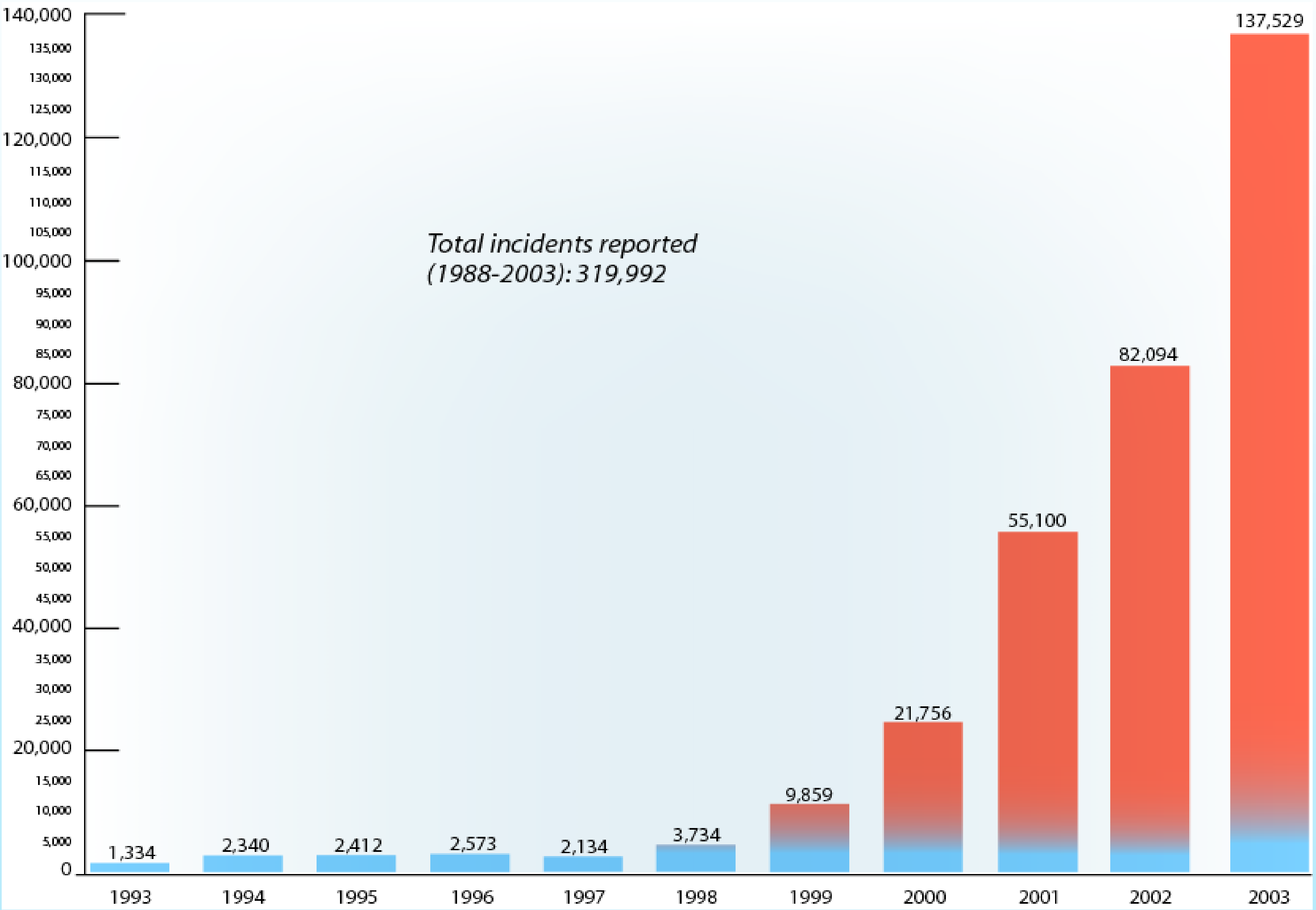
- **Current computing environment was not designed to be secure, e.g.**
  - C language lacks intrinsic bounds checking
  - IP lacks source address verification
  - Border Gateway Protocol highly vulnerable to attacks
  - Operating systems shipped with wide-open services
- **The result is “coping” behavior to deal with intrinsically insecure environment**
  - Constant discovery of new vulnerabilities (mostly network exploitable)
  - Scramble to release and install patches and updates
  - Crackers reverse engineer patches to develop viruses, worms, trojans, etc.
  - Economic loss, embarrassment, denial of service, waste of resources
  - Time window between discovery of vulnerability and launch of attack is shrinking
  - Companies shift risk to customers, e.g. recent Verizon news

Current System Architecture

(Slide from Carl Landwehr, NSF)

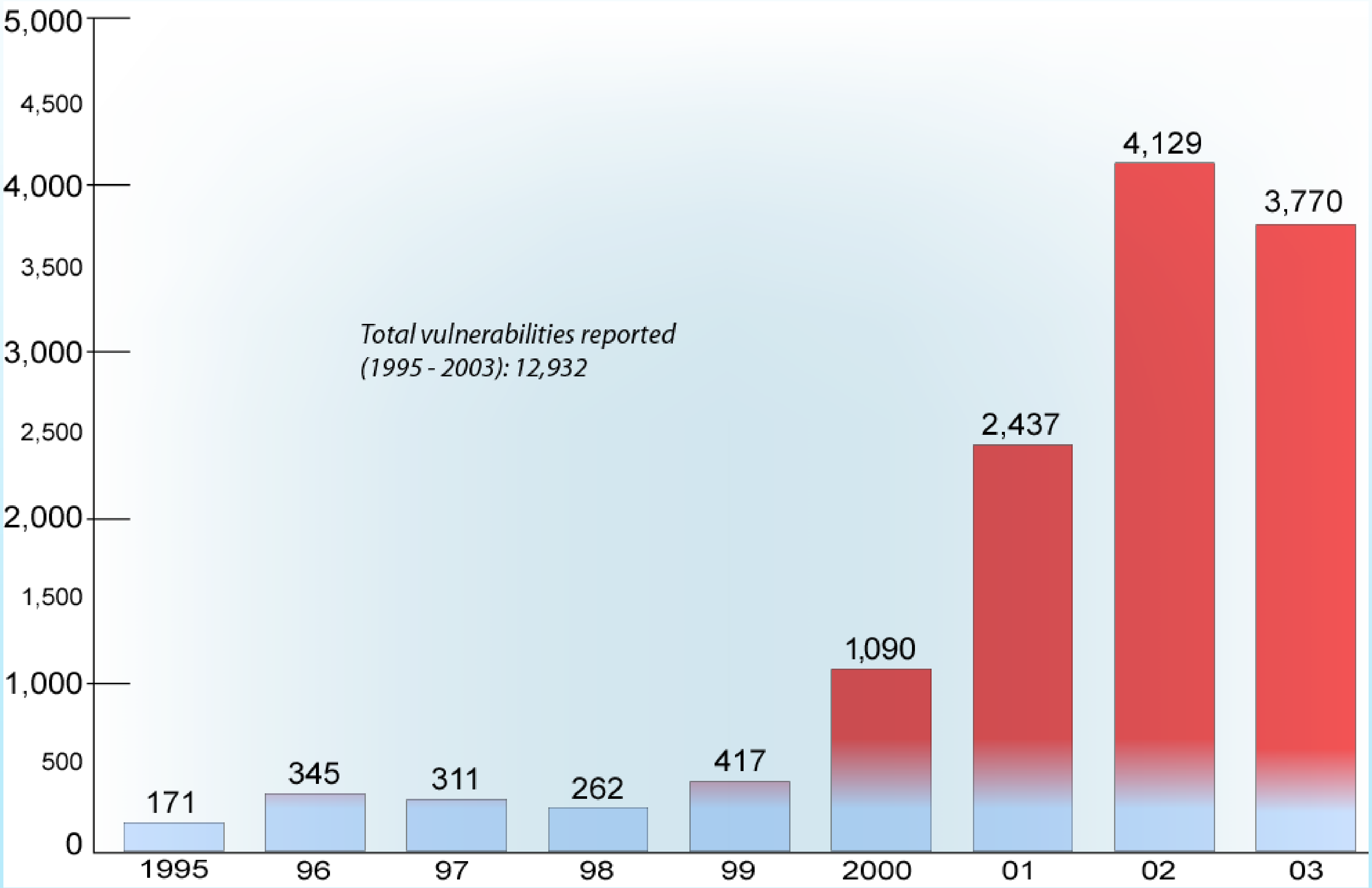


Incidents Reported to CERT/CC
(Slide from Richard Pethia, CMU/CERT-CC)



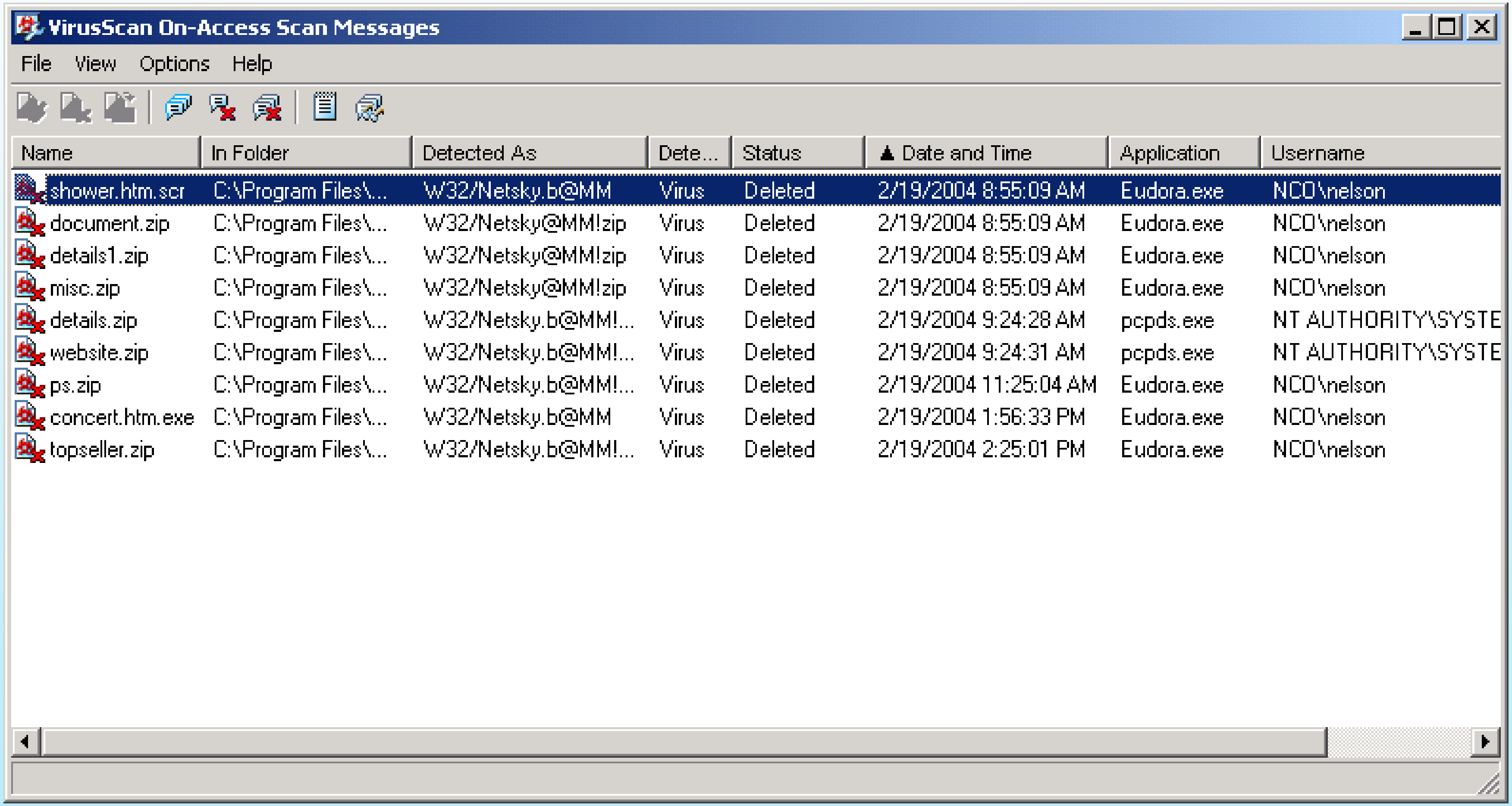
Total incidents reported (1988-2003): 319,992

Vulnerabilities Reported to CERT/CC
(Slide from Richard Pethia, CMU/CERT-CC)



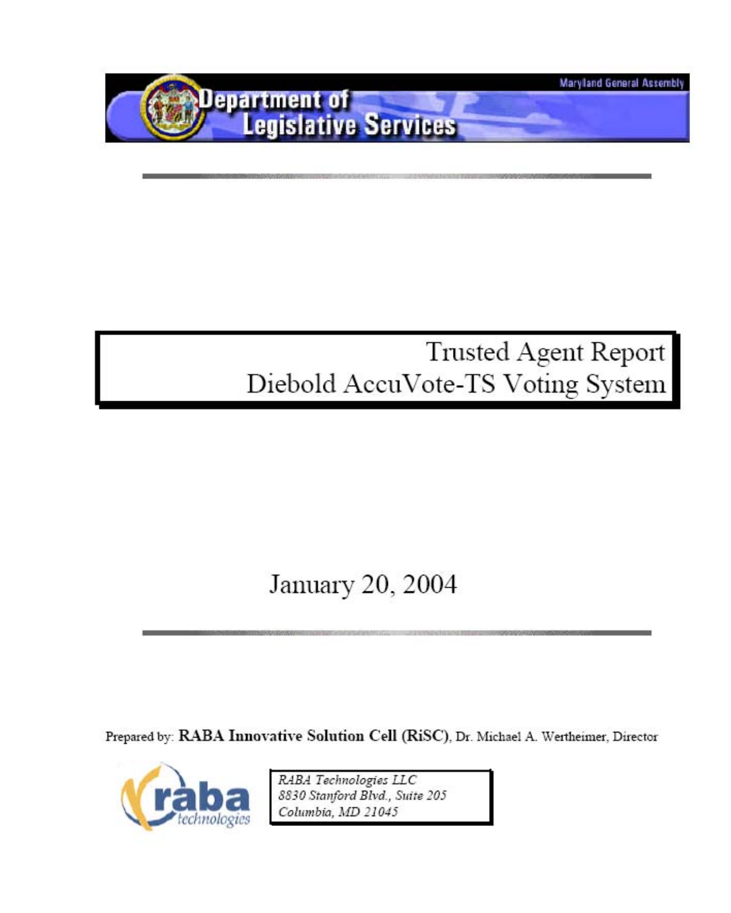
Total vulnerabilities reported (1995 - 2003): 12,932

Recent Personal Example: Netsky virus attacks from infected PCs in major Federal agency



Name	In Folder	Detected As	Dete...	Status	▲ Date and Time	Application	Username
shower.htm.scr	C:\Program Files\...	W32/Netsky.b@MM	Virus	Deleted	2/19/2004 8:55:09 AM	Eudora.exe	NCO\nelson
document.zip	C:\Program Files\...	W32/Netsky@MM!zip	Virus	Deleted	2/19/2004 8:55:09 AM	Eudora.exe	NCO\nelson
details1.zip	C:\Program Files\...	W32/Netsky@MM!zip	Virus	Deleted	2/19/2004 8:55:09 AM	Eudora.exe	NCO\nelson
misc.zip	C:\Program Files\...	W32/Netsky@MM!zip	Virus	Deleted	2/19/2004 8:55:09 AM	Eudora.exe	NCO\nelson
details.zip	C:\Program Files\...	W32/Netsky.b@MM!...	Virus	Deleted	2/19/2004 9:24:28 AM	pcpds.exe	NT AUTHORITY\SYSTE
website.zip	C:\Program Files\...	W32/Netsky.b@MM!...	Virus	Deleted	2/19/2004 9:24:31 AM	pcpds.exe	NT AUTHORITY\SYSTE
ps.zip	C:\Program Files\...	W32/Netsky.b@MM!...	Virus	Deleted	2/19/2004 11:25:04 AM	Eudora.exe	NCO\nelson
concert.htm.exe	C:\Program Files\...	W32/Netsky.b@MM	Virus	Deleted	2/19/2004 1:56:33 PM	Eudora.exe	NCO\nelson
topseller.zip	C:\Program Files\...	W32/Netsky.b@MM!...	Virus	Deleted	2/19/2004 2:25:01 PM	Eudora.exe	NCO\nelson

Another Example: Recent Analysis of State of Maryland Electronic Voting System



Maryland General Assembly

Department of Legislative Services

Trusted Agent Report
Diebold AccuVote-TS Voting System

January 20, 2004

Prepared by: RABA Innovative Solution Cell (RiSC), Dr. Michael A. Wertheimer, Director

raba technologies

RABA Technologies LLC
8830 Stanford Blvd., Suite 205
Columbia, MD 21045

" It is our opinion that the current DIEBOLD software reflects a layered approach to security: as objections are raised additional layers are added. True security can only come via established security models, trust models, and software engineering processes that follow these models; we feel that a pervasive code rewrite would be necessary to instantiate the level of best practice security necessary to eliminate the risks we have outlined in the previous sections. Our analysis lacked the time and resources to determine if DIEBOLD has the expertise to accomplish this task."

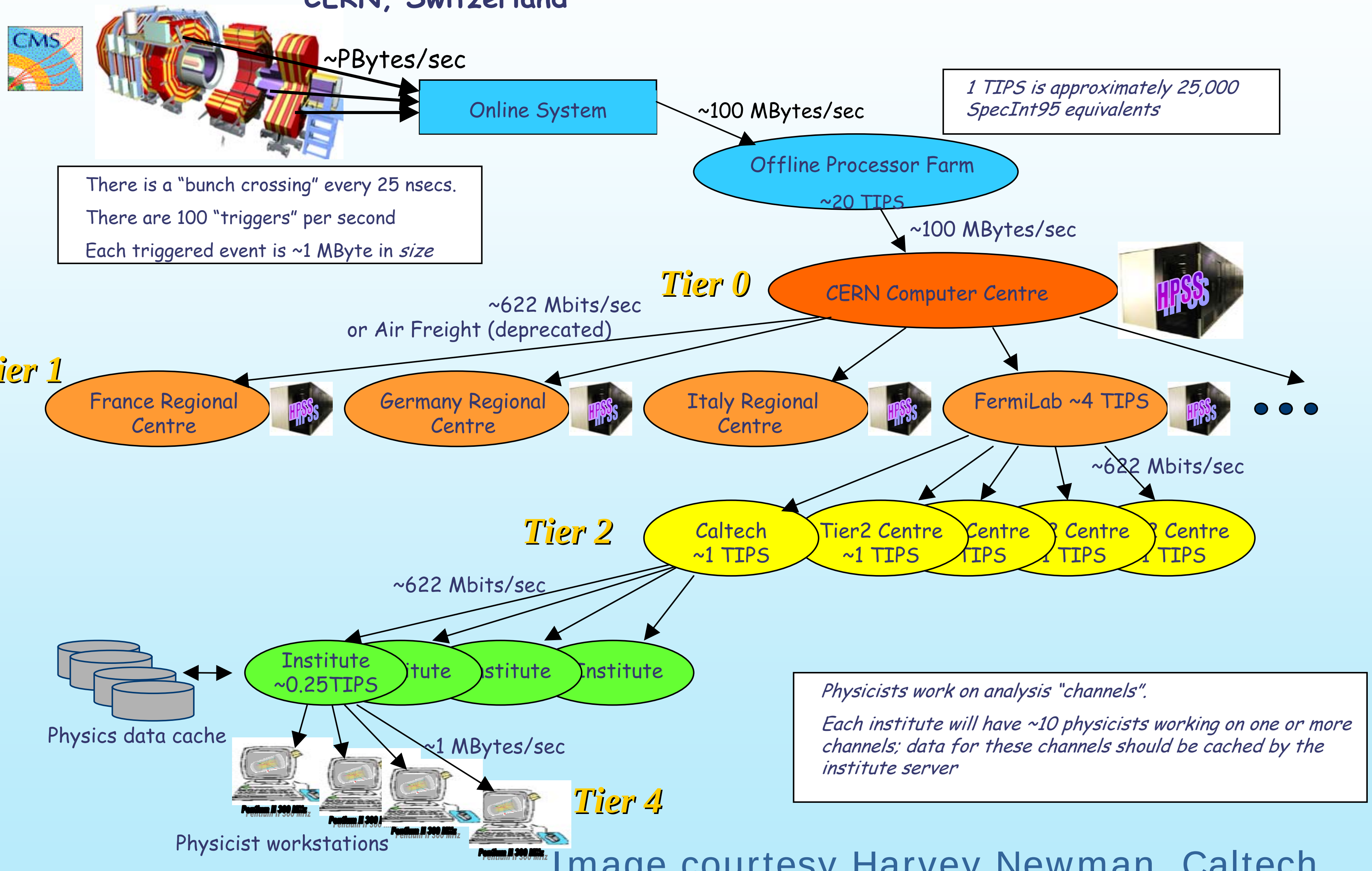
http://mlis.state.md.us/Other/voting_system/trusted_agent_report.pdf

Grid Computing: Example of Middleware to Enable Distributed Computing

- **Goal: Enable a geographically distributed community [of thousands] to perform sophisticated, computationally intensive analyses on Petabytes (10^{15} bytes) of data**
- **R&D supported by federal agencies**
- **Organizations coordinating Grid tools and security**
  - Global Grid Forum www.ggf.org
  - Globus Project www.globus.org
- **Standards: Open Grid Services Architecture, Open Grid Services Infrastructure (uses Web Services)**
- **Globus Toolkit™ centers around four key protocols**
  - *Security*: Grid Security Infrastructure
  - *Resource Management*: Grid Resource Allocation Management
  - *Information Services*: Grid Resource Information Protocol
  - *Data Transfer*: Grid File Transfer Protocol (GridFTP)
- **Several companies have embraced grid concepts, e.g. IBM, HP, Microsoft**

Particle Physics Data Grid

Large Hadron Collider,
CERN, Switzerland



~PBytes/sec

Online System

~100 MBytes/sec

1 TIPS is approximately 25,000 SpecInt95 equivalents

Offline Processor Farm
~20 TIPS

There is a "bunch crossing" every 25 nsecs.

There are 100 "triggers" per second

Each triggered event is ~1 MByte in *size*

~100 MBytes/sec

Tier 0

CERN Computer Centre

~622 Mbits/sec
or Air Freight (deprecated)

Tier 1

France Regional Centre

Germany Regional Centre

Italy Regional Centre

FermiLab ~4 TIPS

~622 Mbits/sec

Tier 2

Caltech
~1 TIPS

Tier2 Centre
~1 TIPS

Centre
TIPS

Centre
1 TIPS

Centre
1 TIPS

~622 Mbits/sec

Institute
~0.25TIPS

itute

nstitute

Institute

Physics data cache

~1 MBytes/sec

Tier 4

Physicist workstations

Physicists work on analysis "channels".

Each institute will have ~10 physicists working on one or more channels; data for these channels should be cached by the institute server

Image courtesy Harvey Newman, Caltech

Security Implications of Grid Computing (1)

- Need to allow access to trusted sources, but how do you determine trust in a dynamic community of thousands (or more) in different organizations?
- Need to allow Web services on port 80 (HTTP) or port 443 (SSL, HTTPS) through the firewall
  - Application level firewalls
- Companies such as IBM, HP, and Microsoft offer commercial grid software and services, but typically only for Intragrids (inside organizations) where security can be managed coherently
- The more interesting security issue is the virtual organization or Intergrid
  - Unsolved problem, because current solutions create Federations of Enterprises based on pair-wise trust agreements; these don’t scale

Security Implications of Grid Computing (2)

- **Today Globus Toolkit uses Public Key Infrastructure for both authentication and authorization**
- **Some experts advocate using PKI only for authentication (based on a certificate authority)**
- **Use directory services for authorization (probably LDAP) with communication through Security Assertion Markup Language (SAML)**
  - Shibboleth is a reference implementation http://shibboleth.internet2.edu
- **SAML is a web-based language (over HTTP) that allows three kinds of messages:**
  - Attribute assertions
  - Authentication assertions
  - Authorization assertions
- **For some transactions we need to add privacy**
  - How to anonymize identity, attributes, actions, and personal data?
  - Anonymity vs. irresponsibility

Why should we care about privacy?

- **History has shown that available information can be abused to persecute individuals with differing beliefs**
  - Nazi Germany
  - Stalinist Russia
  - Maoist China
  - Iraq under Hussein
- **Even in the US**
  - Exile of Nisei from coastal California in WW2
  - McCarthy anti-Communist hearings
  - CIA domestic spying (Church committee hearings of 1973)
- **Laws explicitly safeguard some information privacy**
  - Gramm-Leach-Bliley Act covers privacy of financial records
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers privacy of medical records
  - European Union Directive 95/46 covers protection of personal data

Web Services

- Middleware architecture and program interfaces that enable application-to-application communication
- Run primarily on top of http (or https) web protocols
- Allow aggregation of functions provided by heterogeneous software modules, including legacy apps
- Allow changes to underlying components without manual reprogramming
- Allow seamless extension of functions and services

Security in Web Services is Just Being Developed

- **HTTPS/SSL for secure point-to-point communication with known trusted parties, but**
  - no authorization, auditing, non-repudiation
  - not end-to-end, stops at HTTPS server
  - no digital signature verification through to the data base
- **WS-Security: message level security protocol**
  - persists end-to-end
  - interoperable with web services such as SOAP, SSL, Kerberos, PKI, SAML, etc.
  - http://www-106.ibm.com/developerworks/library/ws-secmap/
- **Managing trust issues is still a challenge**

Emerging Issue of Role-Based Security

- **Role based security: Each of us assumes different roles with different security requirement. One individual may act as:**
  - Manager signing timecards or authorizing procurement
  - Researcher working on data with foreign collaborators
  - Individual buying books from Amazon.com at lunch hour
- **How to handle these different roles using common equipment (PC, network)?**
- **Alternative is separate networks and equipment for each role that requires a different levels of security or access - cumbersome and impractical**

How can research help?

- **Research can identify incremental improvements**
  - Coping with intrinsically insecure environment
- **Research can identify fundamental improvements**
  - Creating intrinsically secure environment
- **Researchers must pay attention to issues associated with implementation**
  - Disruption of existing systems and services
  - Incentives to deploy – ROI
  - Backwards compatibility

We are not idea limited: Examples

- **Concepts of controlled composability**
  - Build up trustworthy systems from secure atoms
  - Both data and function tightly controlled, e.g. using analogy with objects
  - Provable security may not be possible, but probable security may be adequate
- **Concepts for improved network protocols**
- **New classes of SCADA systems with goal of intrinsic security**
- **Improved languages and tools to assure “probable” security**
- **Improved basic theories for dealing with security and reliability**
  - Old example: reliable system from unreliable components (Von Neumann, Moore-Shannon, others)

Role of President's Information Technology Advisory Committee (PITAC)

- **PITAC reports to President through OSTP**
- **PITAC has begun study of Federal cybersecurity research**
  - First public meeting on this topic scheduled for April 13 in Washington, DC
  - Likely will look at both incremental and fundamental research
  - Further information available at http://www.nitrd.gov/pitac/ over next few weeks
  - Public comments will be welcome at

    pitac-comments@nitrd.gov

For Further Information

Please contact us at:

nco@nitrd.gov

Or visit us on the Web:

www.nitrd.gov